



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

AmazCart CMS 3.4 - Cross-Site-Scripting (XSS)

EDB-ID:

51219

CVE:

N/A

EDB Verified: ✘

Author:

[SAJIBE KANTI](#)

Type:

[WEBAPPS](#)

Exploit:   / 

Platform:

[PHP](#)

Date:

2023-04-03

Vulnerable App:



 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPLOIT MANUAL SUBMISSIONS ONLINE TRAINING

```
# Exploit Title: AmazCart CMS 3.4 - Cross-Site-Scripting (XSS)
# Date: 17/01/2023
# Exploit Author: Sajibe Kanti
# Vendor Name: CodeThemes
# Vendor Homepage: https://spondonit.com/
# Software Link: https://codecanyon.net/item/amazcart-laravel-ecommerce-
system-cms/34962179
# Version: 3.4
# Tested on: Live Demo
# Demo Link : https://amazy.rishfa.com/
```

Description

AmazCart - Laravel Ecommerce System CMS 3.4 is vulnerable to Reflected cross-site scripting because of insufficient user-supplied data sanitization. Anyone can submit a Reflected XSS payload without login in when searching for a new product on the search bar. This makes the application reflect our payload in the frontend search bar, and it is fired everything the search history is viewed.

Proof of Concept (PoC) : Exploit

- 1) Goto: <https://amazy.rishfa.com/>
- 2) Enter the following payload in 'Search Item box' :
"><script>alert(1)</script>
- 3) Now You Get a Popout as Alert 1
- 4) Reflected XSS payload is fired

Image PoC : Reference Image

- 1) Payload Fired: <https://prnt.sc/QQaiZB3tFMVB>

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.